What is claimed is:

1. A computing apparatus using SPN structure having a plurality of S boxes and a linear converting unit in an F function, comprising:

a set of bit numbers inputting unit receiving an input of a set $T=\{t_1, t_2, t_3 \ldots t_r\}$ of bit numbers obtained by unequally dividing all bit numbers of input data to be given to the computing apparatus; and

a value indicating existence probability of linear converting unit outputting unit outputting a value A_T indicating an existence probability of an appropriate linear converting unit corresponding to a plurality of S boxes of which input and output bit numbers are equivalent to the divided bit numbers.

2. The computing apparatus according to claim 1, wherein said value indicating existence probability of linear converting unit outputting unit comprises a minimum value determining unit obtaining a minimum value $u_k(k=1, 2, \ldots, r)$ of a sum of elements of a set formed by selecting optional k elements from elements of the set T, and a maximum value determining unit obtaining a maximum value $v_k(k=1, 2, 3, \ldots, r)$ of a sum of elements of a set formed by selecting optional k elements from

elements of the set T, wherein

a value obtained by subtracting a maximum value of k' that satisfies $u_k \geqq v_{k'}$(k'=0, 1, ..., r, v_0=0) for a value k, from k is set as w_k(k=1, 2, ..., r), and the value A_T is obtained by subtracting a maximum value of w_k from a value of (r+1).

3. The computing apparatus according to claim 1, further comprising:

a linear converting unit existence determining unit determining whether the vale A_T is positive, and determining that the appropriate linear converting unit is present when the value is positive.

4. The computing apparatus according to claim 2, further comprising:

a linear converting unit existence determining unit determining whether the value A_T is positive, and determining that the appropriate linear converting unit is present when the value is positive.

5. The computing apparatus according to claim 3, further comprising:

a pseudo MDS matrix forming unit forming as the linear converting unit, a pseudo MDS matrix corresponding

to an MDS matrix in a case where the bits are unequally divided when it is determined that the linear converting unit is present.

6. The computing apparatus according to claim 4, further comprising:

a pseudo MDS matrix forming unit forming as the linear converting unit, a pseudo MDS matrix corresponding to an MDS matrix in a case where the bits are unequally divided when it is determined that the linear converting unit is present.

7. The computing apparatus according to claim 5, wherein the pseudo MDS matrix forming unit sets a matrix M of r columns and r rows to $M=(M_{ij})$ (i=1, 2, ..., r, j=1, 2, ..., r) while setting as an element a partial matrix M_{ij} of t_i columns and t_j rows of which an element is 0 or 1, obtains $c(e)=e+r-A_T+1$ for each positive number from e=1 to (A_T-1), obtains a set $T_1=\{t_{i1}, t_{i2}, ..., t_{ie}\}$ formed by optionally selecting e elements from elements of the set T and a set $T_2=\{t_{j1}, t_{j2}, ..., t_{jc(e)}\}$ formed by optionally selecting c(e) elements from elements of the set T, and obtains a matrix M such that a value of a small matrix of an optional matrix M corresponding to the set (T_1, T_2) and a value of a rank of a small matrix of an optional

matrix M corresponding to the set (T_2, T_1) is equal to either a column number of a small matrix of the matrix M or a number of ranks of a small matrix of a matrix M.

8. The computing apparatus according to claim 5, wherein the pseudo MDS matrix forming unit sets a matrix M of r columns and r rows to $M=(M_{ij})$ (i=1, 2, ..., r, j=1, 2, ..., r) while setting as an element a partial matrix M_{ij} of t_i columns and t_j rows of which an element is 0 or 1, obtains $c(e)=e+r-A_T+1$ for each positive number from e=1 to (A_T-1), obtains a set $T_1=\{t_{i1}, t_{i2}, ..., t_{ie}\}$ formed by optionally selecting e elements from elements of the set T and a set $T_2=\{t_{j1}, t_{j2}, ..., t_{jc(e)}\}$ formed by optionally selecting c(e) elements from elements of the set T, and obtains a matrix M such that a value of a small matrix of an optional matrix M corresponding to the set (T_1, T_2) and a value of a rank of a small matrix of an optional matrix M corresponding to the set (T_2, T_1) is equal to either a column number of a small matrix of the matrix M or a number of ranks of a small matrix of a matrix M.

9. The computing apparatus according to claim 7, wherein a small matrix corresponding to the sets (T_1,

T_2) is configured by a partial matrix designated by columns respectively corresponding to the t_{i1}, t_{i2}, ..., t_{ie} and rows respectively corresponding to the t_{j1}, t_{j2}, ..., $t_{jc(e)}$, among partial matrixes M_{ij} that function as elements of the r columns and r rows to configure the matrix $M=(M_{ij})$.

10. The computing apparatus according to claim 8, wherein a small matrix corresponding to the sets (T_1, T_2) is configured by a partial matrix designated by columns respectively corresponding to the t_{i1}, t_{i2}, ..., t_{ie} and rows respectively corresponding to the t_{j1}, t_{j2}, ..., $t_{jc(e)}$, among partial matrixes M_{ij} that function as elements of the r columns and r rows to configure the matrix $M=(M_{ij})$.

11. A computation method using SPN structure having a plurality of S boxes and a linear converting unit in an F function, comprising:

receiving an input of a set $T=\{t_1, t_2, t_3 \ldots t_r\}$ of bit numbers obtained by unequally dividing all bit numbers of input data to be given; and

outputting a value A_T indicating an existence probability of an appropriate linear converting unit corresponding to a plurality of S boxes of which input and output bit numbers are equivalent to the divided bit numbers.

12. The computation method using SPN structure having an F function according to claim 7, comprising:

determining whether the vale A_T is positive or not; and

determining that the appropriate linear converting unit is present when the value is positive.

13. The computation method according to claim 12, wherein a pseudo MDS matrix corresponding to an MDS matrix in a case where the bits are equally divided is formed as the linear converting unit.

14. A computer-readable portable recording medium used by a computer executing a computation process using SPN structure having a plurality of S boxes and a linear converting unit in an F function, storing a program for causing the computer to perform, comprising:

receiving an input of a set $T=\{t_1, t_2, t_3, \ldots t_r\}$ of bit numbers obtained by unequally dividing all bit numbers of input data to be given; and

outputting a value A_T indicating an existence probability of an appropriate linear converting unit corresponding to a plurality of S boxes of which input and output bit numbers are equivalent to the divided

bit numbers.

15. A computing apparatus in which Feistel structure and SPN structure are combined, receiving data input and setting a computation result for the data input as a data output, wherein

at least one first data converting units that perform data conversion using the Feistel structure, and at least one second data converting units that perform data conversion using the SPN structure are continuously combined between the data input and the data out.

16. The computing apparatus according to claim 15, wherein the SPN structure comprises a nonlinear converting unit having an input/output bit number obtained by dividing a block length of one block of the data input by a word length, and a liner converting unit that uses interleaving conversion.

17. The computing apparatus according to claim 15, comprising:

a nonlinear converting unit having a probability 0 that for a set of input data in which a differential appears only on at least one fixed input bit among input

bits to the nonlinear converting unit, a differential appears for a set of output data in which a differential appears on at least one fixed output bits located at the same location as at least one fixed input bits, and further a probability 1/2 that an optional linear relational equation only related to at least one fixed output bits and at least one fixed output bits, realizes between all the input data and output data 1/2, is provided, as a nonlinear converting unit configuring the SPN structure.

18. The computing apparatus according to claim 16, comprising:

a nonlinear converting unit having a probability 0 that for a set of input data in which a differential appears only on at least one fixed input bit among input bits to the nonlinear converting unit, a differential appears for a set of output data in which a differential appears on at least one fixed output bits located at the same location as at least one fixed input bits, and further a probability 1/2 that an optional linear relational equation only related to at least one fixed output bits and at least one fixed output bits, realizes between all the input data and output data 1/2, is provided, as a nonlinear converting unit configuring the SPN

structure.

19 A computation method in which Feistel structure and SPN structure are combined, receiving a data input and setting a computation result for the data input as a data output, wherein

at least one piece of first data conversion that performs data conversion using the Feistel structure and at least one piece of second data conversion that performs data conversion using the SPN structure are combined to be executed between the data input and the data output.

20. The computation method in which the Feistel structure and the SPN structure are combined according to claim 19, wherein

in first data conversion using the SPN structure, nonlinear conversion of which a number of input bits and a number of output bits are equivalent to a value obtained by dividing a block length of one block of a data input by a word length, and

liner conversion that uses interleaving conversion, are executed.

21. The computing method in which the Feistel structure

and the SPN structure are combined according to claim 19, wherein

nonlinear conversion having a probability 0 that for a set of input data in which a differential appears only on at least one fixed input bit among input bits to be used for the nonlinear conversion, a differential appears for a set of output data in which a differential appears on at least one fixed output bits located at the same location as the at least one fixed input bits, and further having a probability 1/2 that an optional linear relational equation only related to the at least one fixed input bits and the at least one fixed output bits is realized between all the input data and output data, is executed as nonlinear conversion to be executed in the SPN structure.

22. The computing method in which the Feistel structure and the SPN structure are combined according to claim 20, wherein

nonlinear conversion having a probability 0 that for a set of input data in which a differential appears only on at least one fixed input bit among input bits to be used for the nonlinear conversion, a differential appears for a set of output data in which a differential appears on at least one fixed output bits located at

the same location as the at least one fixed input bits, and further having a probability 1/2 that an optional linear relational equation only related to the at least one fixed input bits and the at least one fixed output bits is realized between all the input data and output data, is executed as nonlinear conversion to be executed in the SPN structure.

23. A portable computer-readable recording medium being used for a computer that executes computation of receiving data input and that sets a computation result for the input data as a data output, and storing a program causing the computer to perform, comprising:

combining and executing at least one piece of first data conversion that performs data conversion using Feistel structure; and at least one piece of second data conversion that performs data conversion using SPN structure between the data input and the data output.

24. A computing apparatus using SPN structure having a plurality of S boxes and a linear converting unit in an F function, comprising:

set of bit numbers inputting means for receiving an input of a set $T=\{t_1, t_2, t_3 \ldots t_r\}$ of bit numbers obtained by unequally dividing all bit numbers of input

data to be given to the computing apparatus; an

value indicating existence probability of linear converting unit outputting means for outputting a value A_T indicating an existence probability of an appropriate linear converting unit corresponding to a plurality of S boxes of which input and output bit numbers are equivalent to the divided bit numbers.

A computing apparatus in which Feistel structure and SPN structure are combined, for receiving a data input, and setting a computation result for the data input as a data output, comprising:

at least one first data converting means for performing data conversion using the Feistel structure; and

at least one second data converting means for performing data conversion using the SPN structure,

wherein said first data converting means and said second data converting means are continuously combined between the data input and the data output.